MOBILE BIOMETRICS: MULTIMODEL BIOMETRICS FOR MOBILE PLATFORM

Prof. Mrunali Metri
Asst. Professor(MCA), NCRD's Sterling Institute of Management Studies,Nerul, Navi Mumbai
Email: mrunalimetri@gmail.com

Mr. Nikhil Joshi
MCA Semester-VI, NCRD's Sterling Institute of Management Studies,Nerul, Navi Mumbai
Email:- nikhil.joshi027@gmail.com

Mobile biometrics is used in mobile for authentication, with use of this feature user can access mobile device securely without using PIN (Personal Identification Number) and not give access to others. Mobile devices are theft or loss. A simple and convenient authentication system is required to protect private information stored in the mobile device. Therefore, we propose a multimodal biometric authentication approach using face, finger and voice as biometric traits in this paper. We propose a secure, robust, and low-cost biometric authentication system on the mobile personal device. The low hardware and software cost makes the system well adaptable to a large range of security applications.

Key words- *Mobile devices, multimodal biometrics, face recognition, finger recognition, voice recognition.*

INTRODUCTION

Mobile devices such as smart-phone currently brought users for convenience and flexibility. Moreover, these devices are fast becoming an important part of our lifestyle, because of their increasing computational power, storage capacity and use of various applications. However, the security and privacy issues related to mobile devices are unfortunately becoming a major problem, since they are often exposed in public places such as taxis, coffee houses, and airports, where they are insecure to theft or loss. Along with the value of lost mobile device, users also worry about the exposure of private information. Such as names, addresses, short message, and image, may be stolen. Although, the traditional ways to protected the information are used by PIN (Personal Identification Number) which are easy to implement. Constantly under the risk of being stolen, or forgotten. Therefore, there is a need for offering to the user a more reliable and a friendly way of identification or authentication, and biometrics which is identifying or authenticating an individual based on their distinguishing biological or behavioral characteristics, it rising one of the most popular and promising alternative to solve these problems.

Biometrics, the unique biological or behavioral characteristics of a person, e.g., face, fingerprint, iris, speech, etc., is one of the most popular and promising alternatives to solve this problem. Biometrics is convenient as people naturally carry it and is reliable as it is virtually, the only form of authentication that ensures the physical presence of the user. Although biometric systems require data-capture facilities, modern Smartphone's come equipped with a video camera and microphone. The Mobile Biometrics project exploits these features to combine face, finger and voice biometrics for secure yet rapid user verification.

A major challenge, however, is to capture the signal in a way that isn't confused by day-to-day variations. A face, for example, looks different depending on the expression, and lighting and can change over time (such as when growing a beard), Also a finger, if it will be cut or burn of some accident. Similarly, a voice can sound different depending on the user's health (for example, if the user has a sore throat) and is difficult to separate from background noise in loud environments. We must also make the system robust to spoofing by impostors, for example, ensures that photographs don't fool the system.

BIOMETRIC TECHNIQUES AND SYSTEMS

a. Face Recognition

Face recognition is the initial step for face authentication. Although the detection of the face is an easy visual task for a human, it is a complicated problem for computer vision due to the fact that face is a dynamic object, subject to a high degree of variability, originating from both external and internal changes. This is difficult because faces vary in appearance depending on their shape, size, skin color, facial expression and lighting conditions. Our system must be able to detect all faces regardless of these factors. Ideally, the system should handle different orientations and occlusion, but in mobile verification, we assume the person is looking almost directly into the camera most of the time.

According to one study there are two types of face recognition protocols: face verification and face identification. Face identification is used for matching input identity with registered identity. Face verification is used to authorize proper access. With the system proposed in this research, the cell phone's camera was utilized to capture facial points. Once the data was captured, the system used that information to either activate or deactivate all functions.

Face features. These features can be roughly classified into three ways:

- Traditional: relative position, size, and/or shape of the eyes, nose, cheekbones and jaw.
- Three dimensional: using 3D sensors to capture information about the shape of a face.
- Skin texture: using the visual details of the skin and turning the unique lines, patterns, and spots

apparent in a person's skin into a mathematical space.

b. Fingerprint Recognition

Fingerprint recognition may seem to be a bit more secure because a fingerprint is extremely unique and difficult to mimic. This authentication technique may be the most widely known means of successfully identifying a person's identity and already being used in mobile phones. For example, Sagem MC959 handset in the year of 2000 incorporated a fingerprint recognition system into the back panel. One study used fingerprint authentication for digital signing based on the X.509 certificate infrastructure. A unique feature to this research was the fact that users were able to download third party algorithms to customize protocols. Additionally, this research was conducted using an external USB optical fingerprint sensor and the US National Institute of Standards and Technology Biometric Image Software.

Due to various reasons, some particular users are concerned about touching biometric scanners. To tackle this issue, touch less fingerprint authentication has been developed. For example, proposed to use a camera to capture the user's finger at a distance. Then, the finger image obtained can be isolated from the background and fingerprint features can be extracted for authentication. As fingerprint recognition can provide high authentication accuracy, more and more mobile firms recently started to integrate this technique to developed new phones. In 2011, Motorola came up with fingerprint-based authentication with Atrix phones. More recently, Apple applied the fingerprint recognition to the iPhone 5s in which the home button on this phone is also a fingerprint scanner, while HTC also released the newest Android phone of HTC One Max with a fingerprint scanner.

Fingerprint features. The features can be generally represented in two levels:

- Patterns: including arch, loop, and whorl.
- Minutia features: including ridge ending, bifurcation, and short ridge (or dot).

c. Voice Recognition

This biometric attempt to identify a person who is speaking by characterizing his/her voice. The key point is that each human has different voice signatures, and identical words may have different meanings if spoken with different inflections or in different contexts. Another study used a biometric voice recognition system which exchanged a digital signature token encrypted and confirmed by voice. According to an evaluation study, penetration attempts were made against a voice authentication system using a recorded voice. The results showed an illegal authentication success rate of 89%. As we see here, voice authentication would be easier to breach than fingerprint authentication because any digital recorder could work. That being said, a session key exchanged

during communication and verified by voice is a better solution than just a standard voice recognition method. Given a sound sample captured using the mobile device's microphone, our first step is to separate speech from background noise. As in face detection, however, speech detection is complicated by variation from speaker to speaker (for example, due to characteristics of the vocal tract, learned habits, and language) and from session to session for the same speaker (for example, as a result of having a cold).

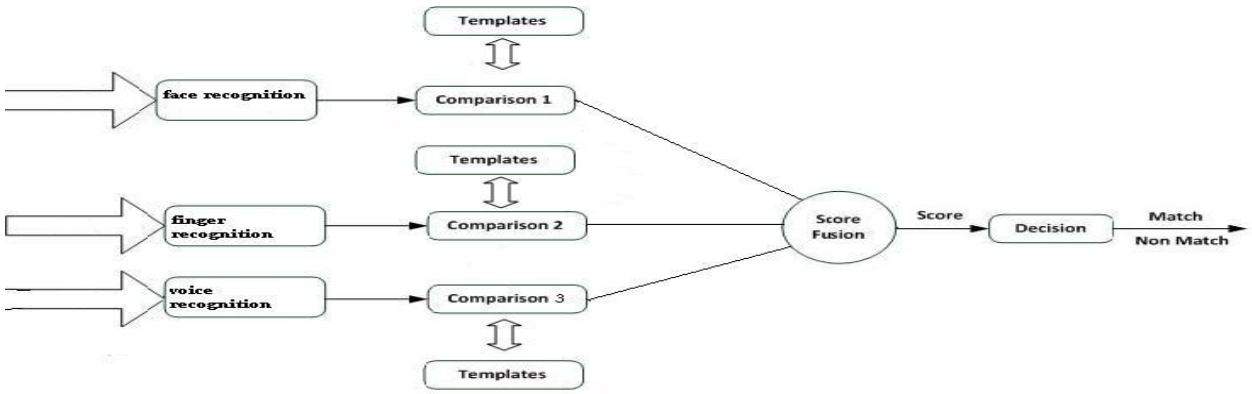
For mobile firms, Apple has developed an application called Siri in 2010 using the voice recognition technology, aiming to answer questions, make recommendations and perform actions by delegating requests to a set of Web services. Then, Lenovo Idea Phone A586 employed a speaker verification system designed by Baidu and A_STAR's Institute for Infocomm Research to look for a specific voice signature, in which the phone can unlock without gestures.

Voice features. The voice biometric authentication systems usually fall into two categories:

- Text-dependent: the text must be the same for enrollment and verification.
- Text-independent: no text constraints during enrollment and verification.

MULTIMODEL BIOMETRICS

In this paper, we combine the results of face, finger and voice authentication to improve system performance. First, it takes sample of their respective biometrics face, finger and voice. After that the new data will be comparing with the store data (templates). Each biometrics compares their data and all comes to the score fusion. In this score fusion data forward to the decision, if its match then it will give access of that device and if it's not match then no access.



PROBLEM WITH EXISTING SYSTEM

a. Performance

In this system we used multimodal biometrics. Single biometrics is easy to use, fast and accurate but when it comes to multimodal biometrics it is slow compare to single biometrics. In multimodal there will be 3 sensors are work together, after scan the data it will be compare and match with other scanners.

b. Accuracy

Accuracy is most important part of biometrics. In face recognition sometimes because of low light, facial expression and beard on men's faces authentication are not possible. In finger recognition, recongnization may be failure because of finger cutting, biometrics sensor does not have quality, and may be of moisture on scanner. In voice recognition pronunciation of words, individual accents, homonyms and unwanted ambient noise.

c. Cost

Cost of multimodal biometrics is high as compare to single biometrics. In these modal three scanners is work together and perform task, because of that 3 equipment multimodal in mobile increase the cost than other devices. When we used device for biometrics it must be high quality device, it help to get accurate and easy detection and access that device.

FUTURE WORK

It would be relevant to use more unique features that are complementary to each other and cover all the characteristics so that behavioral and physiological data are covered for authentication. We also believe that facial expressions detected from the brain waves and the Smartphone camera can be beneficial for increasing the security level of the system. Since they can be used as an extra context trigger.In future works, to enhance the processing time in the mobile environment we have to improved algorithms or optimization processes. Furthermore, we would like to extend this study to consider the effect of variable noise and illumination.

Another research concludes that by incorporating biometrics into a device while establishing a key/lock system (cell phone and charger), theft and intrusion of cell phones would be discouraged. Furthermore, it is important to note that this application can be utilized for any device that requires power. So essentially, if the equipment is separated from its power source and another power source cannot be duplicated without a key or hardware security device, the equipment will be useless.

CONCLUSION

Biometric authentication standards should be implemented to prevent intrusions and theft against mobile cellular devices. To protect these important assets, a system must uses verification other than PIN or password. As we can see from the research above, biometric authentication is a better

alternative, although must be combined with other technology to create better security. Overall, the majority of faces, voices, and fingerprints are not duplicated unless replicated. The only negative aspect to biological and physiological identification is that biometric patterns cannot be revoked, that means, a biological key cannot be changed or altered. If a security system containing biometric, keys was breached, identity theft and other identity crimes could occur. Biometric systems providers will implement more biometric modules, providing more security to the system.

The Mobile Biometrics project aimed to develop a robust and secure verification system for mobile applications (for full technical details and experimental results).The mobile devices is an obvious example where biometric verification can complement (or replace) traditional access methods, such as passwords. Other potential application includes using biometrics to lock and unlock the phone, and mobile money transactions. Biometric authentication still suffers from two major shortcomings: accuracy and speed. It is time-consuming to register and verify biometrics if sensors are not good enough. In order to build a reliable authentication mechanism, we identify that multimodal biometric authentication is better than a single biometric system.

REFERENCES

[1] Juris Klonovs, Christoffer Kjeldgaard Petersen, Henning Olesen, and Allan Hammershøj, (2013). "ID Proof on the Go Development of a Mobile EEG-Based Biometric Authentication System".

[2] Phil Tresadern and Timothy F. Cootes University of Manchester, Norman Poh University of Surrey, Pavel Matejka Brno University of Technology, Abdenour Hadid University of Oulu, Christophe Lévy University of Avignon, Christopher McCool and Sébastien Marcel Idiap Research Institute (January–March 2013) "Mobile Biometrics: Combined Face and Voice Verification for a Mobile Platform".

[3] Carlos Vivaracho-Pascual and Juan Pascual-Gaspar (2012) "On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services".

[4] Qian Tao and Raymond Veldhuis (2010) "Biometric Authentication System on Mobile Personal Devices".

[5] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou (2013) "Surveying the Development of Biometric User Authentication on Mobile Phones ".

[6] Sharath Pankanti, Ruud M. Bolle IBM T.J. Watson Research Center, Anil Jain Michigan State University (2000) "Biometrics:The Future of Identification".

[7] "What is Voice Recognition" (2015). www.webopedia.com/TERM/V/voice_recognition.html

[8] "Speech Recognition"(215). http://en.wikipedia.org/wiki/Speech_recognition

[9] "What is Fingerprint recognition"(2015). http://en.wikipedia.org/wiki/Fingerprint_recognition

[10] "Fingerprint biometrics",(2015). www.imprivata.com/fingerprint_biometrics.